Mehta Decl.
Exhibit D

Sign up and get crypto →

coinbase Cryptocurrencies Learn Individuals Businesses Developers Company Sign in Sign up

Blog Product Company Policy Engineering International Ventures Search

Share

Token Custody Risks: Defining Security in the Crypto World

Tl;dr: This blog builds on our previous blog that provided high-level explanations of Token custody risks. In the following post we dive deeper into defining custody risks for our ERC-20 based tokens and the mitigations that help our security.

By Noama Samreen Engineering, June 29, 2023, 8min read time

Token Recap

Tokens, often issued through smart contracts, represent a variety of digital assets or utilities. They are traded on exchanges with their value often tied to the project or platform they are associated with. Trading involves transferring tokens between wallets, with the ownership change verified and recorded on the blockchain.

However, trading and custody of tokens introduce unique security considerations. In this blog, we once again focus on custody of ERC-20/721 based tokens and NFTs - smart contract assets.

Token Security

Unlike traditional assets, tokens are subject to the code of the smart contract they are based on, which could contain vulnerabilities or malicious functions. Additionally, token transfers depend on the security and integrity of the wallet and exchange infrastructure. Missteps can lead to loss of assets, unauthorized access, or unanticipated behavior of tokens. Therefore, understanding the risks associated with smart contract-based tokens is essential for secure trading and custody.

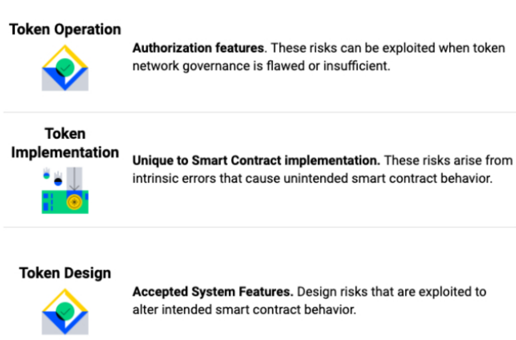
Token Custody

Token custody refers to the practice of holding and safeguarding cryptographic tokens on behalf of their owners. This is essential because the tokens are stored in digital wallets, and the private keys associated with these wallets grant access and control over the tokens. If the private keys are lost or compromised, the tokens can be irretrievably lost or stolen. Custodial services provide a secure solution for token holders by taking responsibility for the safekeeping and management of their tokens.

Our previous blog, How Coinbase reviews tokens on Ethereum for technical security risks provided a high level explanation of the Token custody risk. In this blog, we build on the explanation provided earlier with a deep dive into the specifics of the smart contract code, the design of the token system, and the governance around these assets. In the forthcoming sections, we will explore these risks in detail, illuminating the essential considerations for token developers, traders, and custodians.

Classifying and Decoding the Token Custody Risks

Each smart contract functionality carries a degree of risk due to its inherent nature or potential for misuse. Let's delve into some high-risk features, each scored on a scale from 1 to 5, with 5 indicating a risk so significant that it could disrupt the custody of an asset. Let's quickly recap the classification of token custody risks from our previous blog:



Token Operation

These risks can originate from superuser accounts that might have the ability to alter smart contract functionality, blacklist certain accounts, or confiscate funds from arbitrary accounts. Such accounts may pose a significant threat to the token's decentralization and the security of the user's funds. Key features to look out for in this category include:

- **Blacklisting:** These features can potentially allow a superuser to unfairly target and block certain accounts, compromising access to your assets
  - **Example:** "Alice regularly uses a platform for trading tokens. If Alice's account is blacklisted, she suddenly loses all access to her assets, without any wrongdoing on her part."
- **Confiscating Funds:** This feature enables the removal of funds from any account, a significant violation of security and ownership principles, potentially leading to the loss of your assets without your consent.
  - **Example:** "Bob is a token holder in a network that has confiscate risk. An unethical network admin can arbitrarily decide to remove tokens from Bob's account, leading to a sudden and unexpected loss."
- **Upgrading smart contract:** This feature can allow an entity to change the contract logic arbitrarily, which could alter the rules of how your assets are managed without your knowledge.
  - **Example:** "If an upgrade is applied to a DeFi lending protocol you're using, the interest rates, collateral requirements, or even the basic functionality of your deposited assets could be changed without your consent"
- **Making Unauthorized Transfers:** This risk factor implies unauthorized transfers of assets, a clear threat that could result in unexpected movements of your assets.
  - **Example:** "Carol keeps her tokens in a contract that has this risk. A malicious actor, Eve, exploits this risk to transfer Carol's tokens to her own account, causing Carol to lose her tokens without any action on her part"
- **Minting:** Minting functionality can potentially be misused to flood the market with tokens, devaluing your existing assets.
  - **Example:**"A protocol you're invested in decides to mint a significant number of new tokens. This sudden increase in supply could drastically reduce the value of your existing tokens."
- **Pausing Smart Contract:** If asset functionality or the entire contract can be paused, this could potentially halt your ability to interact with your assets.
  - **Example:** "If a superuser decides to pause the contract, all ongoing and future token transfers would be halted until the pause is lifted. Your ability to trade or move tokens would be temporarily blocked."

Implementation Risks

These risks include the incorrect use of assembly instructions, faulty arithmetic leading to erroneous results, or external calls increasing the complexity and risk of smart contracts. Some of the features in this category are:

- **Using Unique Accounting Logic:** Indicates non-standard logic determining balance changes, which could lead to unpredictable and confusing changes in your asset balance.
  - **Example:** "A DeFi protocol employs a unique, non-standard method for determining balance changes. This might result in sudden, drastic changes in your balance due to unforeseen algorithmic behavior."
- **Using Incorrect or Misleading Arithmetic:** This can lead to inconsistencies in calculations, possibly affecting balance and transactions.
  - **Example:** "The contract contains mathematical operations which do not properly represent the expected business logic of the asset. Known vulnerabilities such as overflows/underflows often result in this issue."
- **Using off-chain Signatures:** Non-standard transaction signatures may not have the level of security and standardization that are typical in the blockchain space, leading to potential vulnerabilities.
  - **Example:** "Imagine a token that implements non-standard off-chain signatures for transactions. An attacker who manages to forge these signatures could potentially create unauthorized transactions, transferring tokens from your account to theirs without your knowledge or consent."
- **Using Assembly Code:** The use of assembly instructions could increase the risk of errors due to the low-level nature of the code.
  - **Example:** "If a token transfer function uses assembly code to perform its operations.a malicious actor familiar with assembly could exploit any vulnerabilities in the code to execute attacks."
- **Rebasing:** If balances and transfer amounts can be adjusted without notification, you might find the amount of your assets changing unexpectedly.
  - **Example:** "A sudden rebase in a token you hold could lead to your balance being adjusted downward, causing a loss of value without any sell-off or market action causing it."
- **Emitting Incorrect Events or Lack thereof:** These indicate potential inconsistencies or missing functionalities related to asset transfers which are fundamental operations for tokens on a blockchain.
  - **Example:** "Consider a token that incorrectly implements the "Transfer" event. This misimplementation might lead to balance changes that do not align with emitted "Transfer" events. For instance, if you send 50 tokens to a friend, but the event reports a transfer of 100 tokens, this could create confusion and potential disputes."

Design Risks

These are the decisions taken while designing the token. Some key design risks include:

- Having No Decimals: Tokens that lack a 'decimals' state variable or function are

indivisible, potentially limiting your transaction flexibility.

- **Example:** "If you hold tokens without a 'decimals' state variable or function, you could be forced to sell or transfer the whole token without the option to transact a fraction of it, leading to inflexibility in managing your assets."

- **Self-destructing Smart Contract:** This feature allows a contract to be destroyed, which could potentially make your assets inaccessible or worthless.
  - **Example:** "A self-destructed smart contract can result in the users losing all the tokens in custody"

In addition to the above identified risks, each user should also follow these four high level guidelines to ensure the most secure experience:

- Due Diligence: Before interacting with a smart contract, conduct thorough due diligence about its features and behaviors. Be wary of features like blacklist, confiscate, and upgrade, as these could disrupt your access to your assets.
- Stay Informed: Regularly monitor the contracts with which you interact, especially those with upgrade or reconfiguration features, as they could undergo changes that affect your assets.
- Understand Transaction Limitations: Some contracts may implement transaction fees or limits (transaction fees, transaction amount limit, time limit on transactions), which could impact your ability to move assets as required. Make sure you understand these limitations before using such contracts.
- Be Aware of Accounting Practices: Non-standard accounting practices could lead to unexpected changes in your asset balance.

Risk Mitigations

In order to address and minimize any previously identified security risks, Coinbase will also apply the corresponding mitigations by working with the issuer or internally. It's important to note that this is not an exhaustive list of our mitigation mappings - rather, a high level overview of the main risks we commonly see.

- Superuser risks
  - Proof of a strong/decentralized governance system,
Proof of strong multisig key practices to execute these operations
A revocation of superuser privileges entirely
- Novel design risks
  - Proof of previous external audits of the design
  - Coinbase creates in-house capabilities to safely support the token contract.
- Similarly, to mitigate the implementation risks in a token contract, we check if the implementation causes unusual behavior by the token contract which cannot be supported by our in-house

Superuser risks

- Proof of a strong/decentralized governance system
- Proof of strong multisig key practices to execute these operations
- A revocation of superuser privileges entirely

Novel Design Risks

- Proof of previous external audits of the design
- Coinbase creates in-house capabilities to safely support the token contract

Unique Accounting (rebasing, fees, threshold transactions, etc.)

- Coinbase exchange engineers backend integrations to support any balance changing, fee logic

Missing Transfer Logic/Events that impact Coinbase's ability to track or manage asset

- The asset issuer needs updates contract to include support required by our exchange

Security First

We hope that by sharing how Coinbase assesses token risks that users may also apply those same principles to make better informed decisions. While these custody risks are just the tip of the iceberg when it comes to smart contract security, we encourage our users and industry partners to perform their due diligence and audits if able.

Engineering

Recent Stories

Company, Dec 10, 2024, 3min read time

Holiday Gifts and Grifts: A Seasonal Safety Guide

Product, Dec 4, 2024

Coinbase One just hit 600,000 members. Here's what's next.

Coinbase One started as a simple subscription in the US that allowed traders to pay zero trading...

Company, Dec 3, 2024, 3min read time

Consumer Protection Tuesday: How to Educate...

coinbase

© 2024 Coinbase

Blog • Twitter • Facebook

United States | English

Company
- About
- Careers
- Affiliates
- Blog
- Press
- Security
- Investors
- Vendors
- Legal & privacy
- Cookie policy
- Cookie preferences
- Do Not Share My Personal Information
- Digital Asset Disclosures

Learn
- Bitcoin Halving
- Ethereum Merge
- Explore
- Coinbase Bytes newsletter
- Crypto basics
- Tips & tutorials
- Crypto glossary
- Market updates
- What is Bitcoin?
- What is crypto?
- What is a blockchain?
- How to set up a crypto wallet
- How to send crypto
- Taxes

Individuals
- Buy & sell
- Earn free crypto
- Wallet
- Card
- Coinbase One

Businesses
- Institutional
- Prime
- Asset Hub
- Commerce
- Derivatives Exchange

Developers
- Developer Platform
- Base
- Staking
- Onramp
- Wallets
- Wallet SDK
- Coinbase App
- Exchange API
- Prime API
- Base Node
- OnchainKit

Support
- Help center
- Contact us
- Create account
- ID verification
- Account information
- Payment methods
- Account access
- Supported crypto
- Status